DEVELOPING A CONTINGENCY PLAN FOR Y2K RELATED COMPUTER DISRUPTIONS OF CRITICAL INFRASTRUCTURES FOR THE SIERRA VISTA FIRE DEPARTMENT

Executive Development

BY: Michael T. Grill
Captain/Paramedic
Sierra Vista Fire Department
Sierra Vista, Arizona

An applied research project submitted to the National Fire Academy as part of the Executive Fire Officer Program

September 1999

ABSTRACT

The Year 2000 computer problem (Y2k) threatens to disrupt critical infrastructures, thereby affecting the Sierra Vista Fire Department's ability to provide emergency services. The problem was the Sierra Vista Fire Department had no contingency plan in order to continue emergency service delivery if Y2k related disruptions were to occur.

The purpose of this research project was to develop a Y2k contingency plan for the Sierra Vista Fire Department.

Historical, descriptive, and action research methodologies respectively were used to answer the following questions:

1. What is the Y2k computer problem?
2. Which critical infrastructures within a community are most susceptible to Y2k-related computer failures?
3. Does the literature identify contingency planning models for emergency service organizations specific to Y2k computer failures of critical infrastructures?
4. What contingency planning model identified in the literature can be adapted to the fire service in order to provide a template for development of a contingency plan for the Sierra Vista Fire Department?

The procedures used for this research included a review of fire service literature, City of Sierra Vista documents, government reports, newspaper and periodical literature. Extensive use of the Internet was employed, as were two informal interviews.

As a result of this research, it was substantiated that the critical infrastructures of electrical power, telecommunications, and water supply are likely to be affected by Y2k-related computer failures.

It was also discovered that a number of Y2k contingency planning models for emergency service organizations existed, with the most useful elements from each combined to create a contingency plan useful to the Sierra Vista Fire Department.

Several recommendations were made, including extensive practice of the contingency plan, sharing results with other fire service organizations, and further research into the topic of Y2k.

TABLE OF CONTENTS

Page

INTRODUCTION

The year 2000 computer problem (Y2k) is an issue receiving worldwide attention. While some experts predict minor disruptions in the delivery of goods and services - similar to a three-day blizzard - extremists are proclaiming TEOTWAWKI: the end of the world as we know it. Despite these widely divergent opinions, there is consensus on one fact: there will be disruptions in basic services and critical infrastructures (Yourdon, 1998). The problem for the Sierra Vista Fire Department is how to continue effective delivery of emergency services if Y2k computer failures negatively impact the community's critical infrastructures.

The purpose of this research was to develop a Y2k contingency plan allowing the Sierra Vista Fire Department to continue effective delivery of emergency services in the event that critical infrastructure failures occur.

A historical research methodology was used to answer the first of four research questions:

1. What is the Y2k computer problem?

A descriptive research methodology was employed to answer the second and third research questions:

2. Which critical infrastructures within a community are most susceptible to Y2k-related computer failures?
3. Does the literature identify contingency planning models for emergency service organizations specific to Y2k computer failures of critical infrastructures?

Finally, action research was utilized to define the answer to the fourth research question:

4. What contingency planning model identified in the literature can be adapted to the fire service in order to provide a template for development of a contingency plan for the Sierra Vista Fire Department?

BACKGROUND AND SIGNIFICANCE

The Sierra Vista Fire Department (SVFD) provides fire and emergency medical services (EMS) for the 39,995 residents of Sierra Vista, Arizona (Cochise College Center for Economic Research [CCCER], 1999). Operating out of two stations, the department employs five administrative personnel, 30 full-time firefighter/EMT's, and 24 part-time paid personnel. Significant to the overall population is the increasing number of retirees relocating from other parts of the country, due in large part to the seasonal climate. At an elevation of 4,680 feet, the January average maximum daily temperature of 58.4 degrees Fahrenheit and 88.6 degrees in the month of July creates an attractive living environment for retirees opting to relocate (CCCER, 1999).

In 1985, the city's fire department was tasked with the development of an emergency operations plan (EOP) whose purpose was to provide for the health, welfare, and safety of the citizens of Sierra Vista in the event of a natural, technological, or war-time disaster (City of Sierra Vista Emergency Operations Plan, 1985). This document specified one full time staff member as the city's emergency management coordinator, whose duties included overall disaster preparedness, management, and revision of the EOP as necessary. However, that position was never funded, and when the city manager decided a revision of the EOP was necessary in 1997, he directed the fire department to coordinate that task. In August of that year, a revision of the plan was finalized and sent to the city manager for his approval. Remaining in that document was a request for staffing the position of emergency management coordinator.

In the fall of 1997, the Y2k computer problem caught the attention of Sierra Vista's city manager. Aware of the potential negative impacts caused by Y2k computer failures, he tasked the city's director of management information services (MIS) to begin assessing the Y2K problem specific to city government.

For the next twenty months, the principal focus of the Y2K remediation efforts revolved around critical information management systems – hardware, software, and the city's mainframe computer. Individual city departments were not asked to assess their Y2K vulnerabilities outside the realm of the personal computers on their desks.

In May of 1998, a document received by the SVFD's planning officer outlined the systemic issues specific to the Y2k computer bug (Petersen, Kellner-Rogers, Wheatley, 1998). Further research culminated in a memo from the department's planning officer to the fire chief descriptive of Y2k issues and concerns regarding negative impacts on the community's infrastructure along with recommendations for action (see Appendix A; fig. 1). Soon thereafter, the fire chief requested the planning officer to begin development of strategies whose purpose would be to ensure continuity of emergency service delivery at the turn of the century.

In July of 1999, the city manager requested a report on each department's Y2k preparedness activities (see Appendix A; fig. 2). Up to this point, he was very pleased with the progress made by the MIS director's efforts to assess, remediate, and test any computer problems within city government. However, he expressed a growing concern that Y2k compliant computer systems should no longer remain the focal issue. Instead, he now maintained that the central issue should switch to emergency preparedness, focusing on the city's ability to provide basic city services, such as law enforcement, fire protection, emergency medical services (EMS), water supply, and other critical infrastructure processes in the event of Y2k-related failures.

The city manager therefore requested department directors to report on Y2k preparedness within their functional areas of responsibility within two weeks. Since the position of emergency management coordinator still remained vacant, he further stipulated both the fire and police departments jointly develop an emergency services Y2k contingency plan to be added as an addendum to the existing EOP. Finally, he requested both agencies prepare and perform a Y2k emergency drill by the end of September, 1999.

The *Executive Development* course at the National Fire Academy includes a module on service quality and marketing. One of the components of this module is a discussion on the dimensions of quality. The term *reliability* is defined in this section as "the frequency with which a product or service fails." Consistent with that definition, this research project seeks to develop a contingency planning process for the SVFD with a goal of ensuring continuity of service delivery in the event Y2k computer disruptions occur.

LITERATURE REVIEW

The literature review for this project focused on three fundamental issues related to the research questions: (1) a historical overview of the Y2k computer problem; (2) identification of critical infrastructure components within the community susceptible to Y2k related disruptions; and (3) identification of existing contingency plans specific to Y2k related disruptions and emergency service delivery.

We learn from Michael Hyatt that the year 2000 computer bug was purposefully introduced at the dawn of the computer age in the late 1940's (Hyatt, 1998, pg. 3). He further characterizes theY2k bug as a "digital time bomb" whose original purpose was to allow computer programmers to save storage space on cumbersome punch cards, which were the precursors of the modern hard-drive (Hyatt, 1998, pg.6). Highlighting this storage problem is a

summary by Kappelman and Scott that "computer storage in 1960 cost ten thousand times or one million percent more than it does today" (Kappelman and Scott, 1997, pp.53-54). The method for saving expensive and valuable storage space was to eliminate the four-digit year entry and replace it with a two-digit year entry. A more in-depth explanation of this process is offered by Anson:

> Years were shortened by lopping off the '19' from the year. A computer would thus read the date as '123199' and know the digits stood for December 31, 1999. What a computer could not do was realize that one second after midnight on that date it would be January 1st, 2000. So, in the manner of an odometer passing 999,999 miles, the numbers would roll back to '00,'which a computer would interpret as 1900 – provided that the sudden loss of a hundred years didn't prevent it from functioning, period (Anson, 1999, pg.37).

Anson also offers an illustration of just how much computer code must be fixed, citing two federal agencies - the Social Security Administration (SSA) and the Department of Defense (DOD) and the daunting task faced by both.

Beginning in 1994, the Social Security Administration hired four hundred programmers to repair 35 million lines of computer code. Finishing three years later, the agency then focused its attention on millions of more lines of code at the state level. This trifled in comparison to what the Department of Defense faced: hundreds of millions of code lines running on more than 1.5 million computers, 28,000 automated systems, and 10,000 networks (Anson, 1999, pg.38)

Unfortunately, Y2k problem is not isolated to just software programming code. Wheatley informs us that microprocessors – known as computer chips and embedded in thousands of systems - are also susceptible to Y2k disruptions:

> Embedded microprocessors are vulnerable to the date change as well. These chips are so prevalent in modern life – in cars, satellites, home appliances, utilities, oil rigs, transportation systems, telecommunications, and medical equipment – that the average American encounters 70 microprocessors by noon each day. There may be 50 billion of these chips in operation. If only 1% of them cannot deal with the calendar change at the year 2000, our society will face large numbers of failures (Wheatley, 1999).

Because of the sheer numbers of embedded chips dispersed throughout the world along with the millions of line of computer code that must be located and fixed, we begin to realize that theY2k problem is really not a technical one; it is more of a problem of inventory. In fact, Vowler tells us that of the seven billion chips shipped in 1996 alone, know one can identify where they all went and if they are Y2k compliant; furthermore there is simply not enough time to locate and test them all prior to the end of 1999 (Vowler, 1997).

To further complicate matters, identical computer chips installed in two different computers but performing identical functions are not equally sensitive to the date problem. In one test where a computer chip failed, its identical twin performed flawlessly (Wheatley, 1999).

If the code is broken and cannot be fixed in time, then it would be important to know what Y2k related failures might occur as a result. It is, however, beyond the scope of this research – as well as unnecessary – to discuss every possible disruption. Therefore, the literature search was purposely narrowed to focus on Y2k disruptions and potential effects on a community's critical infrastructure: electricity, water, and telecommunications (Presidential Decision Directive 63 [PDD63], 1998). This rationale is foundated upon the assumption that if these critical infrastructure processes are unaffected, Y2k becomes a non-event for emergency service providers.

Electricity is crucial to our society, and the literature tells us of the heavy dependency upon computers for the generation and distribution of this resource. Embedded chips are used in every facet of the electrical generation process and have been called the "dirty little Y2k secret" by Rick Cowles, an information technology expert who has worked in the electrical utility industry for over twenty-five years (Cowles, 1997). Seymour concurs, telling us that the power industry's biggest problem is tracking down microprocessors, though no one has any idea how many there are, where they are, or what role they play in power generation and distribution (Seymour, 1998, pg. 160).

Of particular concern are the 103 nuclear power plants supplying 22% of all electrical power in the U.S. - all of which contain thousands of embedded chips (Dolan, 1999). Hyatt states that "of those systems responsible for running critical processes, such as oil production and electrical power, one in five will fail in the year 2000" (Hyatt, 1998, p. 28).

The North American Electric Reliability Council (NERC) is the trade association representative of the energy producers within North America (Yourdon, 1999, pg. 89). According to NERC, the ability of electrical producers to provide uninterrupted service is an interdependent process with the entire power grid only as strong as the weakest link in the chain (NERC, 1998). In other words, the industry will succeed or fail collectively. All producers and distributors of electricity must be Y2k compliant; if not, the entire grid could be jeopardized (NERC, 1998).

A NERC survey revealed that as of the summer of 1999, 70% of suppliers of electricity were Y2k ready, with 24% prepared with limited exceptions (Presidents Council on Y2k Conversion [PCY2K], 1999). This same report tells us, however, that there are several areas of the country that may experience power disruptions of an unknown period because of the local

power supplier not meeting the Y2k deadline (PCY2K, 1999). Many Y2k researchers (Seymour, 1998; Hyatt, 1998, p.70; Mills, 1999) predict disruptions of electrical power in some localities lasting as long as several months.

Telecommunications are a second critical infrastructure component cited in the literature as susceptible to Y2k failures (Hyatt, 1998, pg. 73). Over 92% of Americans receive their phone services from one of seven local carriers; furthermore, only three long distance companies hold over 80% of the market for long distance calls (Guidry, 1999). Similar to the electrical industry, the key to the proper functioning of the telecommunications infrastructure is the ability of each carrier to be Y2k compliant. On August 6, 1998, Joel Willemssen of Congress's General Accounting Office testified to the Technology Subcommittee of the House Science Committee regarding this issue:

> Reliable telecommunications services are made possible by a complex web of highly interconnected networks supported by national and local carriers and service providers, equipment manufacturers and suppliers, and customers. The key is interoperability: all of the pieces must work together (USGAO,1998, page no.unavailable).

As of July 1999, the largest local and long-distance carriers were 98% compliant, meaning just a few systems required fixing. (Federal Communications Commission [FCC], 1999). Because of issues surrounding interoperability, none of these large telephone companies can guarantee customers will not experience any Y2k-related problems. However, they are confident that service disruptions that do occur will be minor and quickly remedied (FCC, 1999).

As in other sectors, there are concerns about the Y2k readiness of smaller companies that have not adopted a systematic approach to addressing the Y2k challenge. Many smaller companies in the communications sector that are working on the problem have completion dates

that are dangerously close to the millennium rollover, leaving little time for vendor delays or other difficulties that may arise in remediation and testing (PCY2K, 1999).

Of particular concern to the fire service is the status of the telecommunications center receiving and forwarding 911 calls. Known as public safety answering points (PSAP's), most are heavily reliant upon computer technology. A survey in June of 1999 revealed that of approximately 2,200 PSAP's responding, only 37% were Y2k ready, with 92% expecting to be Y2k ready by the end of the year (Federal Emergency Management Agency [FEMA], 1999). The survey also revealed that only slightly more than half of the respondents (55%) had contingency plans in place in the event their telecommunications processes failed (FEMA, 1999).

Water is as important to a community as electricity and telecommunications, and obviously has an important role in fire suppression. Almost every community has a water supply system dependent upon electricity. Therefore, losing electrical power will negatively impact the overall water distribution process, forcing back-up power sources into service. Furthermore, many municipal water systems are inundated with software and embedded systems that may not be Y2k compliant (Gasper, Schweig, and Echols, 1997). These computerized systems control not only water distribution; they also regulate the back-flow of lawn fertilizer through residential sprinkler systems, waste in hospitals, and prevent sewer runoff from contaminating drinking water. Evidence of the importance of computerized systems to water utilities and their susceptibility to Y2k related mishaps is illustrated in an event occurring in Van Nuys, California on June 16, 1999. During a Y2k related test, four million gallons of raw sewage spilled into city streets due to the failure of an embedded system to properly close a valve (Felder, 1999).

Similar to the power industry, the water utilities are highly dependent on outside vendors, such as chemical plants, fuel suppliers, and even other water utilities (North, 1998).

Failure to procure product from any of these vendors would cause disruptions and reduction in water distribution capacity.

The literature supports the possibility – or even likelihood – of disruptions in electricity, water, and telecommunications due to Y2k issues. FEMA summarizes this fact and simultaneously urges fire service organizations to develop contingency plans in the event that they occur (FEMA: Contingency and Consequence Management Planning [FEMA - CCMP], 1999):

> The complexity and inter-relationships of the automated systems supporting our critical infrastructure, the global reach of some systems, and the varying rates at which Y2k repairs are being made, make it difficult to accurately predict all the possible Y2k situations we may encounter. With less than a year to go until the century date change occurs, the emergency management community must prepare to minimize the potential impacts of Y2k problems on public safety and health by developing sound contingency plans.

FEMA offers a nine-step Y2k planning model (FEMA-CCMP) emphasizing a community approach to planning. This approach recognizes the resource constraints that would be imposed upon FEMA if Y2k disruptions were widespread. Therefore, this plan advocates the utilization of not only public sector resources, but private sector assets as well in order to sustain communities facing long-term critical infrastructure disruptions.

A second Y2k contingency planning model is described by Caper Jones, in which he identifies nine goals to consider when planning for Y2k disruptions within the context of municipal government (Jones, 1999). Broad in scope, this plan provides a general structure upon which municipalities can begin the contingency planning process.

Included in the plan are suggestions for how to build the contingency planning team as well as a calendar for tracking the planning process.

Ed Yourdon (Yourdon, 1999, pg. 5-9) provides a more specific five-step contingency planning process. This plan is an adaptation of an existing software engineering risk management model emphasizing the need to develop a process that is functional, yet simple to comprehend and implement. Yourdon makes the point that contingency plans need to remain basic to succeed, focusing only on the goal of providing business continuity of the most critical functions of the organization. In doing so, he introduces the concept of triage, insisting that contingencies should be developed for only the most mission critical functions of the organization. He argues there is simply not enough time to develop Y2k specific contingencies for all business functions; therefore organizations should focus on contingency plan development for only those processes deemed most crucial.

Forster, Johnston and Lanza (1998) incorporated elements from both the Jones and Yourdon models to produce the Miami-Dade County, Florida Y2k response plan. Combining the calendar tracking element of plan development from Jones's model with the simplistic five step approach described by Yourdon, this model also suggests that plan development should be decentralized. Specifically, each department within Miami-Dade County was required to assess and develop their own Y2k contingencies using a common template developed by the Office of Emergency Management (see Appendix B). When finalized, each department forwarded their respective plans to the Office of Emergency Management for review and inclusion into the overall Miami-Dade County Emergency Operations Planning Guide.

Only one fire department Y2k contingency plan was found in the literature review. An article in the Amarillo Globe-News (Langton, 1998) established that the city of Lubbock, Texas had performed a Y2k exercise to test their contingency plan. In an informal interview with Lieutenant Mark Ethridge, Training Officer with the Lubbock Fire Department (LFD), I learned that the LFD had developed a Y2K contingency plan annex which was incorporated into the community's EOP (M.Ethridge, personal communication, February 25, 1999). The LFD plan is based on a Y2k worst-case scenario and assumes a loss of telephone and radio communications, water supply, automated fueling sites, electrical power, natural gas service, traffic signals and a substantial increase in rescue calls and false alarms (see Appendix C).

With only one fire department Y2k contingency plan found in the literature, the United States Fire Administration's (USFA) Y2k Information Office was contacted to determine their knowledge of fire departments having Y2K contingency plans. In a telephonic interview with Valerie Dyar, Y2K technical consultant for the USFA, it was determined that the USFA had no information regarding fire department Y2k contingency planning, but had received requests from several fire departments inquiring where such a document might be found (V. Dyar, telephonic communication, August 12, 1999).

Literature Review Summary

The literature review provided insights as to the origin of the Y2k computer bug. It also revealed that there is not enough time to fix all the computer code while simultaneously attempting inventory and fix the estimated 50 billion embedded chips worldwide.

Although the types of Y2k related failures is enormous, only those failures threatening a community's critical infrastructure were researched. One document (Presidential Decision

Directive no. 63, 1998) suggested that the electrical, water, and telecommunications infrastructures were the most vital to a functional society.

The power grid is a highly interdependent, technologically driven system whose susceptibility to Y2k disruptions is high. The severity and location of power disruptions is difficult to predict. However, it seems apparent that some communities will experience power outages.

Telecommunication is dependent on computer technology and therefore vulnerable to Y2k disruptions. Important to the fire service are the PSAP's handling 911 calls; however, just over one-third of PSAP's surveyed recently were Y2k ready.

Water distribution is highly computerized in most communities and also requires electricity in order to operate. Although most water utilities have a back-up power system, that system itself is dependent upon the ability to procure fuel for the generators. Furthermore, the number and types of embedded systems found in water distribution systems create additional susceptibilities to Y2k related failures.

With the critical infrastructures of electricity, telecommunications, and water supply having significant exposure to Y2k-related problems, FEMA advocates contingency planning at a community level. Along with a contingency planning model offered by FEMA, four other models were discovered specific to Y2k contingency planning, with one of those (Lubbock, TX.) specific to a fire agency.

The results of the literature review influenced the decision to perform additional research throughout the development of this paper. The purpose for this was two-fold: first, with the Y2k issue literally generating hundreds of pieces of literature daily, I thought this prudent in order to include only the most current information in this project.

Second, it became apparent that no singular Y2k contingency planning model existed that could be easily adapted to meet the needs of the SVFD. Therefore, it became apparent that the SVFD may have to develop a plan based on the existing models described. In the hopes that another model would become apparent, continued research was deemed necessary.

PROCEDURES

This research employed historical research methodology to define the Y2k computer problem, a descriptive research methodology to describe critical infrastructures susceptible to Y2k-related failures as well as identify existing contingency plans for emergency service organizations, and an action research methodology to develop a Y2k contingency planning model specific to the fire service that can be adapted by the SVFD.

Literature Review

Documents from the City of Sierra Vista were reviewed for historical data specific to emergency planning, as were documents from Cochise Community College's Department of Economics for data regarding economic development within Sierra Vista.

A review of the literature specific to Y2k and the fire service was initiated at the National Fire Academy's Learning Resource Center during February of 1999. A similar review of all literature specific to Y2k was conducted at the Sierra Vista Public Library, including newspaper articles, periodicals, textbooks, government reports, and reports from private research organizations.

Use of the Internet

Extensive use of the world-wide web (WWW) was employed during the literature review, with only those documents having a current Internet address as of August 31st, 1999 included in this research.

Several Y2k specific web sites were monitored on a daily basis for current information regarding this topic, including Y2k News Magazine (http://www.y2knews.com/), Westergaard Year 2000 (http://www.y2ktimebomb.com/), and Coalition 2000 (http://www.coalition2000.org/resources.htm). All three sites compile literature daily specific to Y2k from sources such as newspapers, periodicals, and government reports.

Personal Interviews

Two informal interviews were performed during this project. The first was a personal interview with Lieutenant Mark Ethridge of the Lubbock, TX. Fire Department and occurred on the campus of the National Fire Academy in Building J, Rm.104 on the evening of February 25th, 1999.

The second interview was a telephonic communication during the afternoon of August 12th, 1999 with Ms.Valerie Dyar, a Y2k technical consultant employed by the USFA.

Assumptions

It was assumed that authors cited in the literature review based their findings on their own objective research. Furthermore, it was assumed that both Lieutenant Ethridge and Ms. Dyar have a degree of expertise regarding Y2k and the fire service.

Limitations

There were four limitations associated with this research.

The first limitation was the lack of Y2k literature specific to the fire service. In fact, during the initial literature search conducted at the LRC, only three articles were discovered meeting the search criteria. Since each article was a previous work of this researcher (Grill) and the intent of this research project was to disclose new information, their use was of limited value.

A second limitation of this study was the need to use the Internet in order to thoroughly investigate the topic. Because of this, several pertinent articles archived for inclusion in this study at an earlier date were subsequently discarded because of outdated Internet addresses that were no longer accessible. Furthermore, despite the fact that each Internet address cited was current upon completion of this project, there is no guarantee how long these sites can be accessed. Because of this, research replication by other investigators may be hindered.

A third limitation regarding this research is the dynamic nature of Y2k. The body of knowledge grows daily as the end of the year draws to a close. On several occasions during the literature review, new information appeared dating existing literature already included in this project. The process of including the most current information was time consuming – yet necessary – in order to assure the most accurate results possible. A deliberate effort was made to take the full six-months allowed by the Executive Fire Officer program to complete this research because of this fact.

A final limitation of this research is the subjective nature of the topic. Although it was assumed that all information provided by Y2k researchers is accurate and objective, it is impossible for even the most reputable Y2k expert to measure the affects of an event that has not yet occurred, nor has ever occurred in the history of the world. To that end, every attempt was made to include research information from sources viewed by this investigator as credible.

Definition of Terms

Critical infrastructure: *physical and cyber-based systems essential to the minimum operations of the economy and government, such as energy, telecommunications, water systems, banking and finance, and emergency services.*

Electrical power systems: *a critical infrastructure characterized by generation stations, transmission and distribution networks that create and supply electricity to end-users allowing end-users to maintain normal functionality.*

Water supply systems: *a critical infrastructure characterized by the sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration, cleaning and treatment systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including water runoff, waste water, and firefighting.*

Telecommunication systems: *a critical infrastructure characterized by local and long-distance carriers, cellular networks, satellite service, the Internet, and the millions of computers for home, commercial, academic, and government use.*

Year 2000 (Y2k) compliance: *all applications and systems are capable of correct identification, manipulation, display, and calculation using dates outside the 1900-1999 year range and have been tested as such.*

Mission critical functions: *those functions within a fire service organization whose absence or disruption would cause an immediate loss of life and property within the community. Examples include the ability to receive 911 calls, access an adequate water supply for suppression purposes, and procure fuel for fire apparatus.*

RESULTS

Answers to Research Questions

1. What is the year 2000 computer problem?

The year 2000 computer problem – known asY2k- exists because very few computer systems have been programmed to handle a four digit year. Instead, a two-digit year exists on

millions of files used as input to millions of software applications. Two-digit years were used instead of the normal four-digit year in order to save computer storage space.

Not only is the two-digit year found in computer software applications; the same shortcut was applied when producing microprocessors as recently as 1996. With as many as 50 billion microprocessors embedded in everything from automobiles to power plants, failure of only 1% would wreak havoc on society as we know it. With less than four months before the end of the century, there is simply not enough time to find and repair every line of computer code and microprocessor.

With an understanding of what the Y2k computer problem is, we may now address the second research question:

2. **Which critical infrastructures within a community are most susceptible to year 2000 computer failures?**

The critical infrastructures of electrical power, telecommunications, and water supply are the most critical to a functional society, and all three have been identified as particularly susceptible to Y2k computer failures.

The nation's highly computerized power grid contains thousands of microprocessors vulnerable toY2k computer failures. One expert estimates that 20% of systems critical to oil and power production will fail in the year 2000 (Hyatt, 1998, p.8). NERC, the trade association representative of the power industry, tells us that ***all*** producers of electricity must be compliant. If not, the entire power grid may be jeopardized. Several researchers (Seymour, 1998; Hyatt, 1998; and Mills, 1999) predict disruptions in electrical power in some localities for several months.

The telecommunications infrastructure has been revolutionized through advances in information technology in the past two decades; yet not one local or long-distance carrier within the U.S. could claim Y2k compliance as of July, 1999. Therefore, no guarantee is offered by telecommunication carriers that service will not be affected by Y2k computer failures. Of particular concern to emergency service providers is the status of PSAP's handling 911 calls. Only 92% expect to be Y2k compliant by the end of 1999.

Water systems are a third critical infrastructure with significant exposure to Y2k-related computer failures. All municipal water supply and distribution systems rely upon electricity. This reliance in itself infers the Y2k bug may negatively affect a community's water system. Beyond electrical dependence, however, remains the fact that almost all water utilities are inundated with software and embedded systems requiring assessment for Y2k compliance. The sewage spill in Van Nuys illustrates this point (Feldman, 1999).

Realizing that critical infrastructures will be negatively impacted by Y2k computer failures, focus is turned to answering our third and fourth research questions:

3. **Does the literature identify contingency planning models for emergency service organizations specific to year 2000 related failures of critical infrastructures?**

The literature review yielded five constructs utilized by emergency service organizations in preparation of Y2K related failures of critical infrastructures. Four models were developed for emergency service organizations in general, with one model developed specifically for a fire department.

The first model reviewed was the FEMA Contingency and Consequence Management Plan (FEMA-CCMP, 1999). Comprehensive in scope, the plan argues that government will not be capable of providing emergency relief to all communities if widespread Y2K disruptions occur.

Therefore, a community-based strategy is encouraged, with identification of resources available from the private sector necessary for the plan to be effective.

The second model reviewed was developed for municipal government (Jones, 1999). Broader in scope and less specific in detail than the FEMA plan, Jones places emphasis on building the contingency planning team and creation of a calendar designed to track plan development progress.

The third model contains more specificity of detail and is described by Yourdon (Yourdon, 1999). This model places importance upon the need to develop a plan that is basic and simple, yet functional. One important element in this process is the ability to triage organizational functions, focusing on developing contingencies for mission critical functions only. According to Yourdon, it is unnecessary and impossible to develop contingencies for all organizational functions by the end of 1999; there is simply not enough time to do so.

A fourth model described in the literature is actually a unification of the second and third models described above. Developed by Miami-Dade County, Florida (Forster et.al; 1998), a simplistic approach stressing organizational triage is combined with a project management calendar. A unique element inherent in the Miami-Dade model is the decentralization of plan development, tasking each county department with developing contingencies respective to their areas of functional responsibility. By using a common planning template (see Appendix B), uniformity is ensured throughout the county. The department plans are then consolidated by the Office of Emergency Management for inclusion into the overall Emergency Operations Plan.

The last model reviewed was developed by the Lubbock (TX) Fire Department (LFD) in preparation for a city wide Y2K exercise (see Appendix C). Assuming a worst case scenario, the plan is very specific regarding operational contingencies common to all fire departments.

This model's value to the fire service manager is that it provides examples of how contingencies will actually be performed.

Although a request was made of the USFA's Y2K Information Center for additional fire service organization contingency plans, the USFA was unable to provide any assistance.

4. **What contingency planning model identified in the literature can be adapted to the fire service in order to provide a template for development of a contingency plan for the Sierra Vista Fire Department?**

The literature review established that singularly, none of the five models reviewed satisfied the Y2K contingency planning requirements of the SVFD. Collectively, however, a contingency planning model useful to the SVFD could be synthesized by incorporating useful elements from each (see Appendix D).

Specific elements from each model incorporated into the SVFD contingency plan are identified below:

1. Identification of mission-critical functions (Yourdon, 1998). A contingency planning triage model was created to help differentiate mission-critical functions from overall departmental operations (see Appendix D; sect. I).
2. Fostering team building (Jones, 1999). All management personnel were required to help identify mission-critical functions. Similarly, almost all line personnel were solicited for input when brainstorming contingencies of those mission-critical functions (see Appendix D; sect. II-1).
3. Development of a document stressing simplicity (Yourdon, 1998) thereby increasing the chances of implementing an effective plan (see Appendix D; sect. II-2).

4. Emphasis on developing a plan premised on a worse case scenario (Lubbock model); specifically, assuming the loss of three critical infrastructure components: electrical power, telecommunications, and water supply (see Appendix D; sect. II-3).
5. Identifying and categorization of community resources required for successful plan implementation (FEMA-CCMP, 1999) in the event critical infrastructures are disrupted (see Appendix D; sect. III).
6. Development of a six-step contingency planning template (see Appendix D; sect. IV). This allows for decentralization of plan development, a concept identified as useful in the Miami-Dade County plan (Forster et.al; 1998). Employing a standardized planning template ensures plan continuity when used by SVFD officers when developing contingencies respective to their functional areas of responsibility (see Appendix D; sect's V and VI).

DISCUSSION

The historical overview presented in the literature review clearly indicates that the Y2k computer problem should not be a bolt from the blue to society – or the fire service. Computer experts have been aware of the phenomena for over half a century (Hyatt, 1998). Yet, it has clearly come as a surprise to almost all fire departments – including the SVFD, which first became aware of the scope of the problem in the spring of 1998. Illustrative of this point are the results of an informal survey that occurred at the National Fire Academy in August of 1998 revealing a lack of comprehension of the systemic issues surrounding the Y2K bug (Grill, 1998, pg. 30). Currently, the SVFD culture still grapples with the reality of the potential negative impact of Y2K disruptions on critical infrastructures. I offer three reasons why this is so.

First, the background section of this research paper tells us that it was the City of Sierra Vista's MIS director who was tasked with fixing the problem. Therefore, the Y2K problem is currently viewed as being handled at this level.

Secondly, the MIS department itself was initially focused only on the singular task of upgrading computer hardware and software; this myopic perspective disallowed the opportunity to stand back and attempt to comprehend the interdependent reality of contemporary society – an interdependence woven around our reliance on computer technology.

Finally, the SVFD management team itself cannot reach consensus regarding the impact of the Y2k bug on critical infrastructures, with most believing the event will present similar to an approaching storm that, at the last minute, will veer away, leaving the community unscathed (see Appendix A; fig. 3).

However, the literature review disagrees. Several researchers believe Y2k-related disruptions in electrical power (Seymour, 1998; Hyatt, 1998; Mills, 1999; PCY2K, 1999), telecommunications (FCC, 1999; PCY2K, 1999), and water supply (Gasper et al.; 1997) are possible in some communities.

That failure is categorized as *possible* strikes at the heart of the debate within the SVFD management team. The difficulty of predicting *if*, *where*, and *when* these failures might occur is hindered by the fact that this is an unprecedented event, one with no historical data guiding our decision-making process. Two points pertinent to this uncertainty bear mentioning at this juncture of the discussion.

First, Y2k has created a leadership paradox – especially for those in a leadership role within government and public safety organizations.

On the one hand, if the leader takes Y2k-related disruptions seriously, opting to spend public funds on preparedness activities and *no Y2k-related disruptions manifest*, detractors believing Y2k is a hoax created by greedy consultants hoping to cash in on Y2k hysteria may accuse that leader not only of being fiscally irresponsible, but of being a fool, as well. Paradoxically, if the leader decides Y2K-related failures are a non-issue, subsequently failing to develop preparedness plans and Y2k-related failures *do occur*, allegations will focus on the leaders apparent lack of vision and concern for public safety, since 'everyone knew that Y2k was coming, yet you [the leader] did nothing to prepare.' In other words, the fool label still applies.

The second point concerning the uncertainty of Y2k-related disruptions taking place focuses on 'what is at stake' versus 'what is the risk.' If all computer systems were to fail simultaneously, the literature is clear on the impact to society: civilization as we know it would change forever. Therefore the stakes are *extremely high*. However, *what is the risk* such an event will occur?

The SVFD management team is divided when it comes to this question. Will Y2k be the first ever-scheduled global disaster? Or will it be a non-event instead? It may not be pleasant for fire service leaders to identify and contemplate the stakes, and apparently many would prefer not to do so (Grill, 1998, p. 30). It is also easier to ignore the stakes if we conclude the associated risks of an event occurring are unlikely. Yet, it is impossible to prove that Y2k poses zero risk to critical infrastructures, as the literature review informs us.

While the SVFD management team cannot agree what course of action is appropriate, the city manager clearly recognizes which actions would be inappropriate: failure to prepare for Y2k related disruptions.

Simultaneously, he plainly comprehends that his personal opinion of the risk plays no role when it comes to an event that – if it were to occur in an unprepared community – could have catastrophic results. Furthermore, while acknowledging the leadership paradox, he obviously perceives there is only one choice in light of what is at stake: prepare contingency plans in anticipation of critical infrastructure disruptions. To his credit, the SVFD's chief officer predicted the city manager's decision months before it was made, requesting the department's planning officer to begin development of a contingency plan for Y2k-related disruptions.

The third research question attempted to discover existing contingency plans specific to Y2k-related disruptions. Five models were discovered, with one specific to the fire service. It was decided to combine elements from each model in order to construct an appropriate contingency planning document for the SVFD. Each model will be briefly reviewed here as to why it was deemed inappropriate in and by itself for adoption as a useful construct for our agency.

The FEMA (FEMA-CCMP, 1999), Jones (Jones, 1999), and Miami-Dade County models (Forster et al., 1998; Appendix B) were all perceived as overly comprehensive, requiring planning information deemed unnecessary for our agency. Furthermore, each model's broad scope required valuable time to not only triage out unnecessary data elements, but inordinate amounts of time to train personnel in plan implementation. The model introduced by Yourdon (Yourdon, 1999, pg. 5-8) was rejected for the opposite reason: it was too narrow in scope. The Lubbock Fire Department developed a Y2k contingency plan (see Appendix C) specific to a fire agency. Differences in departmental and community characteristics made adoption of the entire plan unrealistic for our community. However, several specific elements – such as communication contingencies – were suitable and readily adaptable for use by the SVFD.

As noted in the results section of this project, the action research employed to answer the fourth research question yielded an effective and useful contingency plan for the SVFD (see Appendix D) which is an amalgamation of useful elements from each of the five models discovered in the literature. Although contingencies have yet to be developed for each mission-critical function and the plan has yet to be tested in an exercise, members from both the SVFD and the Sierra Vista Police Department have commented that this document meets the needs of both organizations and should minimize any impacts Y2k-related disruptions have on our community.

RECOMMENDATIONS

The fact that a computer glitch as unintentional and uncomplicated as Y2k can have such devastating affects on critical infrastructures ushers in a new era of vulnerability to our society: cyber terrorism. Presidential Decision Directive 63 clearly outlines our reliance on cyber-based information systems in order to provide basic services (PDD63, 1998). To that end, five recommendations are offered fundamental to this research paper.

The SVFD should continue to develop the contingency plan constructed from existing models (see Appendix D) for *all* mission-critical functions in the event critical infrastructure disruptions occur. It is important the SVFD management team recognize this is not a one-time contingency plan to be discarded after January 1st, 2000. Rather, this plan will become an integral part of the current emergency operations document in anticipation of the escalation of cyber-related disruptions during the next decade.

A second recommendation is to practice the plan - as directed by the city manager. A precursor to a Y2k drill would be the development of an exercise scenario highlighting the types of problems that might occur if Y2k-related disruptions manifest (see Appendix E).

A third recommendation is to attempt to transform the culture of the SVFD management team specific to Y2k-related disruptions. A high degree of skepticism remains as to whether or not Y2k is an event that should be occupying the time and resources of our organization. Although it can be difficult to change perceptions regarding a deeply held belief, the fire chief must continue to endeavor to do so. Strategies to accomplish this might include beginning each staff-meeting with Y2k as the initial topic. Furthermore, all pertinent articles discovered by the fire chief should be forwarded to each manager, with an informal follow-up discussion of those articles at each staff meeting.

A fourth recommendation is to continue prospectively researching Y2k issues, as the topic is a dynamic and evolving event. This can be accomplished through the Internet, as well as communicating with the USFA's Y2k consultants on a weekly basis in an attempt to discern new information the moment it becomes available.

Finally, since many fire service organizations are currently scrambling to develop a similar contingency planning document, every attempt should be made to share with those departments the results of this research.

REFERENCE LIST

Anson, R.A. (1999, January). The y2k nightmare. *Vanity Fair*. No. 461; p. 25-33.

Cochise College Center for Economic Research. (1999). *Economic focus.* Sierra Vista, AZ: Cochise Community College.

City of Sierra Vista. (1999). *Emergency operations plan.* (pg. 2). Sierra Vista, AZ.

Cowles, R. (1997, October). Embedded logic and controls. *Utilities and the Year 2000*. (electronic edition). Online [WWW]. http://www.accsyst.com/writers/embedded.htm. Accessed May 1st, 1999.

Dolan, D.P. (n.d./1999). *Beyond the hype: likely Y2K impacts on U.S. electricity service*. Online [WWW]. Available at http://www.year2000.com/y2kcurrent2.html. Accessed August 4th, 1999.

Federal Communications Commission. (1999, July 27th). Telecommunications near Y2K readiness. (FCC Publication No. 2210). Online [WWW]. Available at http://www.usia.gov/cgibin/washfile/display.pl?p=/products/washfile/topic/global&f=99072703.ggi&t=/products/washfile/newsitem.shtml. Accessed August 8, 1999.

Federal Emergency Management Agency, United States Fire Administration, National Fire Data Center. (1999, July). Nationwide Y2K 911 readiness report. Online. [WWW]. Available at http://www.usfa.fema.gov/y2k/index.htm#nationwide Accessed July, 1999.

Federal Emergency Management Agency, United States Fire Administration, National Fire Data Center. (1999, June). Contingency and consequence management planning for year 2000 conversion. Online [WWW]. Available at http://www.fema.gov/y2k/cpguide.doc Accessed July, 1999.

Felder, D. (1999).Y2K test causes huge sewage spill.Online [WWW]. Accessed August 18, 1999 Available at http://www.cbs2.com/news/stories/news-990617-081237.html

Forster,L., Johnston, B., Lanza, C. (1998, November). Miami-Dade County Y2K response planning. Online. [WWW]. Available at http://www.y2ktimebomb.com/CP/Organizational/clanza9845.htm Accessed July, 1999.

Gasper, J., Schweig, B., Echols, M. (1997). North Platte, Nebraska: A case study of the year 2000 computer problem. (Tech. Rep. No. 16). Omaha, NE: Creighton University, College of Business Administration. Online [WWW]. Available at http://genteel.creighton.edu/y2k.htm#CaseStudy Accessed August 8, 1999

Grill, M. (1998, December). Will the millenium bug bite you? Fire Chief, 42 (12), 30-33.

Guidry, R. (1999, April 30). Koskinen rides again. Y2K News Magazine. 2 (21), pg. 25.

Hyatt, M.S. (1998). The millenium bug: how to survive the coming chaos. Washington, D.C.: Regnery Publishing, Inc.

Jones, C. (1998). Year 2000 contingency planning for municipal governments. Online. [WWW]. Available at http://www.angelfire.com/mn/inforest/capersj989.html Accessed July,1999.

Kappelman, L., Scott, P. (1996, October). What management needs to know about the year 2000 computer date problem. *Com.Links Magazine*. Online. Available at www.comlinks.com/mag/kapsco1.htm; Accessed February 15, 1999.

Langton, E. (1998, October 1). Lubbock develops respect for the Y2K problem. Amarillo Globe-News. Online. [WWW]. Accessed October, 1998. Available at http://www.amarillonet.com/stories/100198/new_149-2894.001.shtml

Mills, D. (1999, April 9). More guesses the days after 2000-01-01. Westegaard 2000: Powerful Prognostications. Online [WWW]. Available at http://www.y2ktimebomb.com/PP/RC/dm9914.htm Accessed August 8, 1999.

North American Electric Reliability Council. (June 12, 1998). Y2K coordination plan for the electricity production and delivery systems of North America, phase one: June-September 1998 initial assessment and coordination. Online [WWW]. Available at http://www.nerc.com/y2k/y2kplan.html Accessed November, 1998.

North, G. (1998, October 12). Nearly compliant small water utility faces domino effect. Online. [WWW]. Available at http://www.garynorth.com/y2k/detail_.cfm/2840 Accessed August 12, 1999.

Petersen, J.L., Kellner-Rogers, M., Wheatley, M. (1998). The year 2000: social chaos or social transformation. The Berkana Institute. Online [WWW]. Accessed August 23, 1999. Available at http://www.berkana.org/frame.html?4_1_1

President's Council on Y2K Conversion. (1999, August). Third quarterly report. Online [WWW]. Available at http://www.y2k.gov/new/3rdquarterly.html. Accessed August 6th, 1999

Presidential Decision Directive 63. (1998, May). The Clinton administration's policy on critical infrastructure protection. Washington, DC. U.S. Government Printing Office. Online [WWW].Available at http://www.info-sec.com/ciao/paper598.pdf Accessed November 1998.

Seymour, J. (1998.) What to do about the year 2000. PC Magazine. Vol 17; No.17. p.160.

United States General Accounting Office. (1998, August). Serious problems remain in resolving year 2000 and computer security problems. (GAO Publication No. AIMD 98-251). Washington, DC: U.S. Government Printing Office.

Vowler, J. (1997, May 8th). The heart of embedded systems. *Computer Weekly*. Online [WWW]. http://www.computerweekly.co.uk/cwmain/cwmainfram.asp. Accessed May 21st, 1999.

Wheatley, M. (1999, Winter). When complex systems fail: new roles for leaders. *Leader to Leader.* No.11. Online [WWW]. www.pfdf.org/leaderbooks/121/winter99/wheatley.html. Accessed August 5, 1999.

Yourdon, E., Yourdon, J. (1999). Time bomb 2000. (2nd ed.). Upper Saddle River, NJ: Prentice-Hall

Appendix A

Y2K Interdepartmental Correspondence

Figure A1: Y2k Awareness and Concerns

M E M O R A N D U M

DATE: **August 6th, 1998**

TO: **Bruce Thompson, Fire Chief**

FROM: **Mike Grill, Planning Officer**

SUBJECT: **Y2K Awareness and Concerns**

I have been researching the Y2K issue for the past 2 months by reading articles appearing daily in periodicals, newspapers, and conferences devoted to that issue. Here's what I've learned so far:

1. **The Y2K issue is real**. The Gartner Group Inc., a computer industry research group, estimates that U.S. businesses will spend between $125 to $250 billion dollars to remediate the software/hardware issues affected by Y2K. General Motors alone is expected to spend over $500 million. If corporations are taking this issue seriously enough to spend that kind of money, then I suggest this problem is not mythological in origin or just an attempt by unscrupulous software vendors to take advantage of a simple data processing error.

2. **Widespread electric, utility, and telecommunication failures will still occur despite computer networks being 100% compliant.** This is because at the center of this technical time bomb are the embedded microprocessors – 70 billion in existence – that sustain the world's manufacturing and engineering base. They exist in traffic lights, elevators, water, gas, and electrical control systems, medical equipment, and navigation systems. Your car has about two dozen of them. Many of these chips are not date sensitive, but a great number are. Engineers looking at these chips don't know for sure which is which. Further, tests have shown that two chips of the same model installed in two different computers but performing the same function are not equally sensitive to the year end problem. One shuts down and the other doesn't.

   The solution for most companies – and perhaps the City of Sierra Vista – has been to junk their computer systems and replace everything. That's great if you can afford it. But it will not solve the

problem. That's because our community is interdependent upon many vendors and suppliers of goods and services critical to our mission. For example, consider the following entities and the impact on Sierra Vista if they are not compliant:

- Sulfur Springs Valley Electric Co-Op
- Southwest Gas
- Bella Vista, PDS, or Arizona Water
- US West Telephone
- Sierra Vista Community Hospital
- Various financial institutions within our community

Does our city have any data telling us what state of compliance these organizations have achieved? What about other key agencies our community depends upon in order to perform its mission? Are we exploring this issue? Should we help them achieve compliance? Can we help them achieve compliance?

3. **There is a lack of knowledge within our community of the seriousness of this problem.** In general, two categories of response can be noted. First, most people view the problem as affecting only a few industries, such as finance and insurance. These people also understand that it may affect their organization, but their information technology department "is on top of it".

The second category of reactions is that human ingenuity and genius will solve this problem. If a software developer claims to have created a program that can correct all systems (and there have been quite a few of those lately) he is believed. After all, he's just what we've been expecting and hoping for.
Regardless of your belief of the seriousness of this problem, one thing is clear: we are dealing with an immutable deadline. It is not as if we are preparing for some disaster that may occur. We know that this is going to happen. We just are not sure how bad it will be.

Consider what Senator Robert Bennet (R-Utah) had to say on July 15th, at a National Press Club luncheon. Bennet, Chairman of the Senate Special Committee on the Year 2000 stated that " We have reached the point where we cannot solve the whole problem. That is very clear. As a nation, as a government, we cannot get this problem solved. So what we have to do is start making priority choices. To go back to the medical term, we have to do triage".

Senator Bennet also stated the following beliefs:

- There will be brownouts and regional blackouts, but the power grid as a whole will not go down.
- Water systems in most communities will function, but there will be some municipalities where they will fail – and in those communities he predicts serious problems.
- Serious problems will exist in health care, including lack of Medicare reimbursement to hospitals and clinics, wreaking havoc on their financial situation. Also, medical instruments are expected to have serious problems and hospitals far enough away from other facilities will have no backup, creating a serious health care problem.
- Riots might occur in regions where welfare and other government checks are not issued due to the computer glitches.

Certainly, any or all of these problems are a potentiality within Sierra Vista. Therefore, I would like to make the following recommendations in order to help our community survive this problem with minimal impact on life and property:

1. Our city's leaders must begin right now to create the resources for groups of people and businesses to come together in conversations revealing how we might lessen the impact of this situation. Education is key. We must be honest and straightforward with the community as to the potential serious nature of this problem. Secrecy must be replaced by full and frequent disclosure of information. The only way to prevent driving our citizens into isolated and self-preserving behaviors is to entrust them with difficult – even fearsome – information, and then insist that we work together.
2. Leaders can do this by providing the time and resources for people to assess what is critical for our local government to sustain its mission, functions, relationships, and overall quality of life.

3. The City of Sierra Vista must assess where it is most vulnerable and develop contingency plans for disruptions or loss of service for:

- All utilities – electricity, water, gas, phones
- Food supplies
- Public safety
- Healthcare
- Residents most at risk, e.g. the elderly and those requiring medication

This assessment and planning should not occur within individual locales (our city) but in geographic regions (Cochise County). These activities can be initiated by civic organizations such as Lions or Rotary, Council of Churches, Chamber of Commerce, etc.

4. Each city department should focus on assessment and contingency plans including:

- How the organization will perform essential tasks in the absence of present systems
- How the organization will respond to failures or slowdowns in information and supplies
- What simplified systems can be developed now to replace existing ones
- Relationships with suppliers, customers, other communities – how we will work together

Chief, I would like to discuss this document and our emergency preparation plans for this potential problem at your earliest convenience.

Figure A2: E- mail memo regarding Y2K Emergency Preparedness Meeting

Mike,
[City Manager] wants to have a meeting on the City's Y2k planning on July 21st at 1000 in the City Hall Conference Room. Basically, the purpose of the meeting is to discuss the interaction between departments. I plan to go, and would appreciate it if you can make it too. I realize it's relatively short notice, so just let me know if you can't be there. Thanks!

Bruce

Bruce Thompson
Fire Chief
Sierra Vista (AZ) Fire Dept.

Figure A3: Memo Regarding Results of Y2K Meeting

Mike,

As for the Y2k meeting, it went all right. The cops are doing pretty well in terms of the IC role, and have laid out some responsibilities that we'll plug names into at our next meeting. All in all, I think we're pretty well covered. I still think this will be a non-event on the order of Hurricane NORA a few years back, magnified exponentially.

Talk to you when you get back.

Appendix B

Miami-Dade County Y2K Contingency Planning Criteria

The Miami-Dade County Office of Emergency Management (OEM) suggests that this document be used when developing Y2K contingency plans. Following these guidelines should help each entity consider most facets of a possible Y2K related incident. Also, following this format will facilitate the review process by the OEM.

These criteria are not intended to limit or exclude additional information that an entity may decide to include in their plans.

This form may be attached to your plan submission to the OEM. You may use it as a cross-reference to your plan by listing the page number where the criteria are located in your plan. This will facilitate an accurate review of your entity's plan by the OEM. You may also choose to use the page indicator spaces as a place to check off each issue after it has been addressed.

Name of entity: _____

I. **General Information:** Provide basic information concerning the entity to include:
   A. Name of the entity, address, telephone number, emergency contact telephone number, fax number, and e-mail address.
   B. Name, address, telephone number, emergency contact telephone number, fax number, and e-mail address of contact person and alternate contact person.
   C. Organizational chart identifying key management positions in place during emergencies.

   Page: _____

II. **Plan Introduction:** Provide an introduction to the plan that describes its purpose and the desired outcome that will be achieved through the planning process. Also provide any other information concerning the entity that has bearing on the implementation of this plan.

   Page: _____

III. **Identify Threats:** Describe potential problems that may occur if there is a disruption in each of the following services. There is another category entitled "Increased demand" which pertains to stresses on an entity due to an increased demand for their goods or services. Plans should account for two time frames: Less than one week and greater than one week.

A. Electricity Page: ____
B. Natural Gas Page: ____
C. Energy (i.e. fuel) Page: ____
D. Data processing Page: ____
E. Water Page: ____
F. Sewage Page: ____
G. Communications (telephone, hand held radio, etc.) Page: ____
H. Transportation Page: ____
I. Electronic payment (e.g. ATM, credit cards, etc.) Page: ____
J. Other goods or services pertaining to your entity Page: ____
K. Increased demand Page: ____

IV. **Evaluate and assess the likelihood of a disruption and the impact of that disruption should one occur:** Assessing the likelihood of a disruption may not be applicable to all entities, however each entity should project the impact of a disruption if one occurs.

A. Electricity Page: ____
B. Natural Gas Page: ____
C. Energy (i.e. fuel) Page: ____
D. Data processing Page: ____
E. Water Page: ____
F. Sewage Page: ____
G. Communications (telephone, hand held radio, etc.) Page: ____
H. Transportation Page: ____
I. Electronic payment (e.g. ATM, credit cards, etc.) Page: ____
J. Other goods or services pertaining to your entity Page: ____
K. Increased demand Page: ____

V. Indicate what procedures will be taken to monitor potential disruptions:

A. Electricity Page: ____
B. Natural Gas Page: ____
C. Energy (i.e. fuel) Page: ____
D. Data processing Page: ____
E. Water Page: ____
F. Sewage Page: ____
G. Communications (telephone, hand held radio, etc.) Page: ____
H. Transportation Page: ____
I. Electronic payment (e.g. ATM, credit cards, etc.) Page: ____
J. Other goods or services pertaining to your entity Page: ____
K. Increased demand Page: ____

VI. **Specify actions, if applicable, that may eliminate the disruption in advance:**

VI. Specify actions that may be taken to minimize the impact of disruptions if they materialize:

Appendix C

Lubbock Fire Department Y2k Contingency Plan

Revised Jan.29, 1999

Assumptions: The following assumptions may or may not come about as a result of changing to the year 2000. Our plan is based on a worst-case scenario, hoping for the best.

1. We are assuming that we could loose the use of all telephone lines and radio repeaters.

2. We are assuming that there could be a loss of water supply.

3. We are assuming that we will not have use of the automated fueling sites.

4. We are assuming that we will not have electrical power for an extended period of time.

5. We are assuming that we will not have natural gas fuel for an extended period of time.

6. We are assuming there will be numerous rescue calls (elevators), numerous false fire alarms and loss of traffic signals.

These assumptions could completely happen all at once or could only partially happen. Therefore, we must be prepared to handle the worst case scenario and be flexible enough to adjust the plan as needed to the level that these assumptions may occur.

Resources:

1. Water Supply
   A. Water Department will have all of the above ground tanks full of water Dec. 31, 1999.
   B. All Mutual Aid Departments will be contacted by the Operations Deputy Chief and put on alert for the possible need of their tankers.

C. Water Tankers will be manned and strategically located to cover the city. Water Tankers will be dispatched to all confirmed structure fires.

D. Portable Water pumps from the Street and Water Departments will be mounted on Engines that do not have hard suctions on them or carried by each DC.

E. Drafting sites will be pre-planned by each of the engine companies prior to Dec. 15th, 1999.

F. Normal fire hydrant operations will be conducted until it is determined there is no water available from them. At that time, water will be used from the tankers.

2. Fuel

Shop personnel will man the fuel truck on the night of Dec. 31, 1999. The fuel truck will be full and ready to respond by noon Dec.31, 1999. Refueling of the fuel truck can be done at the Municipal Hill fuel site. Fuel rounds will be made on an as needed basis.

B. Fleet Services will provide two transport tankers, one filled with diesel, the other gasoline. One of the units will be capable of refueling from underground fuel sites. Emergency Services units will be priority for fuel usage.

3. Monitoring Equipment

A. All four gas monitors and AIMS 3250's will be fully charged

and tested Dec. 26, 1999.

B. All CDV-777 radiological monitors will be tested and batteries checked Dec. 26th, 1999.

4. Equipment

A. All officers will use the following schedule to check equipment if they are not involved in an emergency response. These are listed in priority order:

12:02am:	Truck Operation	Then, every 30 min. for 2 hours.
12:03am:	PA System	Dispatch will initiate PA check.
12:04am:	Phones	Then, every 30 min. for 2 hours.
12:05am:	Radio Check	Dispatch will initiate.

The following will be checked by the officer in charge and reported to the EOC as soon as possible:

Cell phones
Generators
Gas monitoring equipment
Pagers

B. In the event that you are unable to make the previous checks, due to an emergency response, please complete them as soon as possible to ensure continuation of service to the community. Contact the EOC with the results.

5. Personnel

A. All first line equipment will be fully staffed (four personnel).
B. Reserve engines, reserve truck company and Heavy Rescue will be staffed with four personnel. Brush 3 and Brush 5 will have an equipment operator and firefighter.
C. Additional personnel will be assigned to each station to act as a contact point for the general public and communications for EOC and the equipment assigned at the station.
D. All off-duty District Chiefs' and Command Assistants will report to the Mobile Command Post, at a pre-designated location, to assist Command.

Appendix D

Sierra Vista Fire Department Y2K Contingency Plan

Section I). Identify Mission Critical Functions

The Sierra Vista Emergency Services Organizations (SVESO)– police, fire, and EMS - have certain functions critical to perform in order to protect property and minimize loss of life, injury, and illness. It is essential to identify these **Mission Critical Functions (MCF's)** specific to the SVESO's.
As an example, the following represents a list of many of the MCF's, including, but not limited to:

1. ***Receiving 911 calls from the public***
2. ***Ability to receive emergency dispatches from the Public Safety Answering Point (PSAP)***
3. ***Providing law enforcement activities***
4. ***Providing fire suppression***
5. ***Providing EMS response***
6. ***Responding to fire and security alarm activations***
7. ***Ability to call-back additional personnel when needed***

As a first step in Y2K contingency planning, therefore, it is necessary to identify the MCF's specific to our emergency service organizations. This can be accomplished through a triage process using the **model on the following page**.

It is important to remember to include all of your management staff when performing the triage process. The critical question to ask is this:

"IF WE COULDN'T _____, THEN IMMEDIATE LOSS OF LIFE, P ROPERTY, INJURY, AND ILLNESS WOULD OCCUR."

For example, "if we couldn't **receive alarms,** then immediate loss of life, property, injury, and illness would occur."

The following page depicts a model useful for categorizing all functions, followed on the following page by a worksheet that will be useful in identifying our most important MCF's.

Contingency Planning Triage Model

Mission Critical systems and items whose failure would cause *immediate* loss of life, property, injury, and illness.

Systems and functions that are not currently Mission Critical, but whose failure could eventually result in loss of life, property, injury, and illness.

Systems and functions that are "nice to have," but whose failure would not result in loss of life, property, injury, or illness.

Y2K Contingency Planning Triage Worksheet

"IF WE COULDN'T _____, THEN IMMEDIATE LOSS OF LIFE, PROPERTY , INJURY, AND ILLNESS WOULD OCCUR."

Mission Critical Functions

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

11._____

12. _____

Section II.)

Brainstorm Contingencies for Each Mission Critical Function

At this point we should 'brainstorm' how MCF's might be provided in the event of a critical infrastructure disruption caused by Y2K. Several key points need to be mentioned.

1. Include as many people on the front-lines of service delivery as possible in this process. They are the ones most familiar with the day-to-day operations on how MCF's are actually provided in the field. They possess amazing ingenuity, creativity, and are your most valuable resource at this stage. Including them will also create the buy-in necessary to ensure the plans actually work while simultaneously reinforcing the fact that Y2K disruptions are very possible and should be taken seriously.

2. Remember: the more complex the plan, the less effective it is likely to be. So, remember the ***KISS*** principle: Keep It Simple Stupid!

3. Finally, we should hope for the best, but prepare for the worst. Therefore, the following **5** assumptions should be made specific to Y2K contingency planning for the community of Sierra Vista:

- The loss of all telephone lines and radio repeater systems;
- The loss of water supply – or at the very least – a diminished water supply;
- The loss of electrical power for an unknown period of time;
- The loss of natural gas services for an unknown period of time;
- Panic buying on certain items – gasoline, water, etc. - towards the end of the year.
- An increase in police, fire, and EMS call volume between December 30th, 1999 and January 31st, 2000.

Starting with the MCF's identified on the previous page under the red circle, ask this critical question:

If the above assumptions regarding Y2K failures become reality, how might we perform the Mission Critical Function/service of _____ if the way we currently perform it fails?

A contingency planning worksheet is provided on the following pages.

Section III). Y2K COMMUNITY RESOURCE GUIDE

The following list is designed to begin a dialogue process with other city departments or local businesses with a goal of determining what resources they can make available – and how those resources might be used – by the SVESO's in the event of critical infrastructure disruptions caused by Y2K failures.

I. Public Sector/Local Government Resources

A.) Name of Department: _____

1. Contact Person: _____

2. Phone/Pgr #: _____

3. Resources Available:_____

4. How Resource is to be used:_____
_____
_____

B.) Name of Department: _____

1. Contact Person: _____

2. Phone/Pgr #: _____

3. Resources Available:_____

4. How Resource is to be used:_____
_____
_____

C.) Name of Department: _____

1. Contact Person: _____

2. Phone/Pgr #: _____

3. Resources Available:_____

4. How Resource is to be used:_____
_____
_____

D.) Name of Department: _____

1. Contact Person: _____

2. Phone/Pgr #: _____

3. Resources Available:_____

4. How Resource is to be used:_____
_____
_____

I. Private Sector/Local Business Resources

A.) Name of Department: _____

1. Contact Person: _____

2. Phone/Pgr #: _____

3. Resources Available:_____

4. How Resource is to be used:_____
_____
_____

B.) Name of Department: _____

1. Contact Person: _____

2. Phone/Pgr #: _____

3. Resources Available:_____

4. How Resource is to be used:_____
_____
_____

C.) Name of Department: _____

1. Contact Person: _____

2. Phone/Pgr #: _____

3. Resources Available:_____

4. How Resource is to be used:_____
_____
_____

Section IV). Contingency Planning Worksheet

If the assumptions regarding Y2K disruptions become reality, how might we perform the Mission Critical Function/service of _____ if the way we currently perform i t fails?

Contingency Plan for _____

1. *Criteria for invoking the plan:*

(What would have to happen requiring our agency to implement this plan?)

_____

_____

_____

2. Roles/Responsibilities/Authority

(Who within our agency is responsible for implementing this particular plan? What are their responsibilities? How do we contact them? Who is their back-up in case this person is unavailable?)

_____

_____

_____

3. Resources required for this plan to work

(What resources from inside and outside your agency willbe required in order to successfully operate this plan? This can include personnel, materials, supplies, communications equipment, etc.)

_____

_____

_____

Contingency Planning Worksheet

4. Procedures for Operating in Contingency

(Document steps for implementing the contingency plan)

_____

_____

_____

5. Estimated Cost of the Plan

(Document expected costs of the plan if invoked)

_____

_____

_____

6. Testing the Plan

(Some plans may require only a 'running through' of the list of resources you may need; others may require an actual hands-on experience)

_____

_____

_____

Section V). Contingency Plan for Loss of Water Supply

1. *Criteria for invoking the plan:*

(What would have to happen requiring our agency to implement this plan?)

On December 31st, 1999, the Emergency Operations Center (EOC) will be staffed with personnel identified as necessary for emergency service operations. In the event of power loss, a fire department officer within the EOC willl contact the local water company with inquiries as to their performance capabilities. This will have been discussed and planned with water company representatives prior to this date. If water company states they have lost ability to provide adequate water supply, then plan will be invoked.

2. Roles/Responsibilities/Authority

(Who within our agency is responsible for implementing this particular plan? What are their responsibilities? How do we contact them? Who is their back-up in case this person is unavailable?)

Assistant Chief Frank Capas will be tasked with this responsibility. He will liaison with the water company and be responsible for procuring the resources necessary for the plan to function, plan all testing of the plan, and designate an alternative in the event he is unavailable. AC Capask will be on-duty at the EOC on the night of December 31st, 1999. Contingency plan will be developed by September 15th, 1999 with testing completed by October 31st, 1999.

3. Resources required for this plan to work

(What resources from inside and outside your agency willbe required in order to successfully operate this plan? This can include personnel, materials, supplies, communications equipment, etc.)

Public Works will be inventoried and use of all water tenders and drivers will be necessary on 12/31/99. All water tenders will be filled that day. This will allow the department to have (xxxxx) gallons of water plus the 2000 gallons carried collectively on the fire department apparatus. Our community has a large number of swimming pools that may be used for a static water supply. We will use a floating pump to quickly fill our apparatus at locations pre-designated throughout the community. This will required public education, cooperation, and a significant amount of pre-planning. Also, coordination with Parks and Rec will ensure that the swimming pool at Veterans Memorial Park has not been drained and that access is available.

4. Estimated Cost of the Plan

(Document expected costs of the plan if invoked)

We no longer carry hard-suction on our apparatus; therefore, it will be necessary to purchase a portable floating pumps @400 gpm each. This will cost $1,500 ; We will also require at least 10 additional personnel on-duty during this period of time for water shuttle operations. In-direct costs will include the use of personnel from other city departments for this operation as well as compensation (?) to other community resources required in this operation.

5. Procedures for Operating in Contingency

(Document steps for implementing the contingency plan)

For a 12 hour period prior to midnight on 12/31/99, all city water tenders will be located either Station 1 or Station 2. All personnel will be on stand-by, and other department personnel (public works drivers, etc) will be staffed in the appropriate firehouse or other designated location yet to be determined. E11 will be staged at Veterans Park along with the submersible pump. If the plan is invoked, a shuttle system will be used with uncommitted fire apparatus serving to shuttle water from the pool(s) to the fireground. The public works water tenders will be used as a water storage facility on the fireground itself. Mutual Aid will be invoked as necessary and if available.

6. Testing the Plan

(Some plans may require only a 'running through' of the list of resources you may need; others may require an actual hands-on experience)

We will initially hold a table-top exercise for all involved personnel in September. In October, an actual hands-on drill will occur with conditions be simulated as realistically as possible. A debriefing will occur following this exercise. Finally, another table-top exercise will occur in the first week of December.

Section VI.) Contingency Plan for Loss of 911 System

1. *Criteria for invoking the plan:*

(What would have to happen requiring our agency to implement this plan?)

At 2330 hrs. and every 15 minutes afterwards until 0800 on January 1st, 2000 a department officer within the emergency operations center (EOC) will contact the PSAP (Public Safety Answering Point) with inquiries as to their performance capabilities. This will have been discussed and coordinated with the PSAP prior to this date. If contact is not made, the plan will be invoked.

2. Roles/Responsibilities/Authority

(Who within our agency is responsible for implementing this particular plan? What are their responsibilities? How do we contact them? Who is their back-up in case this person is unavailable?)

Lt. Tom Alinen will be tasked with this responsibility. He will liaison with the PSAP, the communities public education officer, (Marie Hansen) and the local medical community and be responsible for procuring the resources necessary for the plan to function. He will implement testing of the plan and designate an alternative in the event she is unavailable. Lt. Alinen will be on-duty at the EOC on the night of December 31st, 1999. Captain Ken Kimmel will be the back-up assistant for this plan. Contingency plan will be developed by September 1st, 1999 with testing completed by October 31st, 1999.

3. Resources required for this plan to work

(What resources from inside and outside your agency willbe required in order to successfully operate this plan? This can include personnel, materials, supplies, communications equipment, etc.)

The local amateur radio club (RACES) will be contacted and requested for service in the event of a 911 disruption. Their mobile radio units will be strategically located at the following locations: the EOC, each fire station, the police station, and Sierra Vista Regional Health Center. Public works will have every vehicle available, including garbage trucks, street sweepers, etc. strategically posted in areas of the community and within radio range of the ham operators. They will communicate with the ham radio operators with walkie-talkies (approximately 2 mile range of service). Approximately 10 walkie-talkies will be required. On December 1st, 1999, public service announcements (PSA's) will begin education of the public of how to access emergency services in the event of a 911 failure, including locations of posted city vehicles.

4. Estimated Cost of the Plan

(Document expected costs of the plan if invoked)

Costs include, but are not limited to, : 20 walkie-talkies @$130/piece, overtime costs for city employees (approximately $10,000, depending on the length this contingency plan is used; rehab and support for the ham radio-operators (approximately $500).

5. Procedures for Operating in Contingency

(Document steps for implementing the contingency plan)

Beginning December 1st, PSA's will educate the public as to what they should do in the event that a 911 failure occurs. These will be aired over the radio, on public TV, in the CITY COLUMN section of the newspaper, and on the city's Website. Brochures will be distributed that include this information, as well. All city employees identified as critical to plan operation will be on-duty the night of December 31st from 1700hrs until 0800 in the morning. The community center will be the central location where these employees will be staffed until the contingency is invoked. Pizza, soft-drinks, TV, games, and other non-alcoholic refreshments will be provided. It is encouraged that the families of these employees families attend, also. The amateur radio operators and their families will be asked to attend, as well. Once the plan is invoked, employees and radio operators will immediately re-locate to their pre-assigned locations. Once in place, each employee will do a radio/equipment check with each fire/ambulance station and between one another.

Back-up equipment will be placed in the EOC in the event of an equipment failure. As requests come-in for emergency services to these 'remote outposts' that outpost will immediately contact the EOC, whereupon the EOC will contact the appropriate resource to handle that event.

6. Testing the Plan

(Some plans may require only a 'running through' of the list of resources you may need; others may require an actual hands-on experience)

We will initially hold a table-top exercise for all involved personnel in October. In November, over a weekend, an actual hands-on drill will occur with conditions be simulated as realistically as possible. A debriefing will occur following this exercise. Finally, another table-top exercise will occur in the first week of December.

Appendix E

Sierra Vista Fire Department Y2K Exercise Scenario

Purpose: To provide the SVFD with a disaster exercise specific to problems within the community that may be experienced due to the transition into the Year 2000. This exercise will help prepare the SVFD to handle emergency calls for service from **September 1st, 1999 through March 31st, 2000, which has been defined by FEMA as the Y2K transition period. It is important to note that the Federal Response Plan will be in affect during this transition period.**

Assumptions: The following assumptions may or may not come about as a result of changing to the Year 2000. This exercise is based on events that could occur due to computer failures throughout the region as well as predictions by the federal government, including FEMA.

1. We could lose the use of all telephone and radio communications;
2. There could be a reduction in or total loss of water supply;
3. We could lose electrical power to the community for an extended period of time;
4. We could lose our supply of natural gas for an extended period of time;
5. There will be an increase in calls for fire alarm activations;
6. Y2K related disruptions will not be localized to the city of Sierra Vista; therefore, mutual aid from other departments cannot be counted upon, nor can assistance from state or federal agencies.
7. Due to the unique nature of this particular New Year's Eve, off-duty personnel may opt not to respond to call backs because of prior plans, which may include the consumption of alcohol.
8. This exercise represents events that may happen during any 24 hour period during the transition period.

December 31, 1999

Staffing: St. 1: 4 personnel
St. 2: 4 personnel
(based upon current leave schedule)

1445: An assault occurs at Safeway Supermarket

BOX 16 – EMS ASSIGNMENT; INJURED PERSON; SAFEWAY STORE

Rationale: People have been panic-buying, and some items are not to be found in most stores. This is an argument over an item that two people want.

1703: A fire alarm is reported activated at SAIC

BOX 12- ALARM ACTIVATION- SAIC- BUFFALO SOLDIER TRAIL AND AVENIDA COCHISE;

Rationale: Many alarm systems are not Y2K compliant (see list of such systems given to Inspector Clawson). Their embedded chips have internal clocks that fail at 0000 Greenwich Mean Time, which is 1700 local time.

1713: Power goes off in the entire city.
Rationale: same as above regarding embedded chips and local time.

1720: An MVA occurs at the 90/92 intersection
BOX 22-EMS-962-90/92; PD ON SCENE STATES THERE ARE 3 INJURIES;
Rationale: No traffic signal is functioning due to loss of power.

1747: Loving Hands Care Center personnel stops by Station 2 to inform personnel that none of their oxygen generators are functioning and they have 2 patients who need bottled oxygen.
Rationale: Oxygen generating equipment need electricity to function; there is not one nursing home in SV that has a back-up generator on their site.

1825: Power is restored to the west end of the city, but the east end is still without electricity. SVPD and St. 1 have service restored, but not St. 2.
Rationale: Unpredictability of power grid.

1915: SVPD dispatch is overwhelmed with calls from anxious citizens wanting to know what is going on. Also, the 911 lines are busy, mostly from curious citizens not calling in emergencies, but instead calling to see if the 911 system is still functioning.
Rationale: Some people tend to panic!

1956: Another assault is reported, this time at Fry's Food Store

BOX 21-EMS-INJURED PERSON-FRY'S FOOD STORE

Rationale: Another argument over the last 5 one-gallon distilled water bottles left in the store.

2030: Numerous calls from the media making inquiries.

2114: The power once again goes off throughout the entire city;

2130: Power is restored to the entire city.

2210: A police officer stops by St. 1 and St. 2 to inform personnel that the radio and CAD systems has gone down for an unknown period of time. St. 1 personnel attempt to call St. 2 per procedure and discover the telephone systems are also not functioning.
Rationale: Telecommunications is unpredictable during this time period.

2234: SV dispatch receives a walk-in request for an ambulance at 4170 Avenida Paloma for an elderly woman having chest pain.
Portable CB radio's used to dispatch appropriate units

BOX 23-EMS-CHEST PAIN-4170 AVENIDA PALOMA

Rationale: No Y2K relationship

2310: SVPD requests an ambulance stage one block away from 2815 Golden Eagle Drive due to a large millenium party that has become violent, with reports of gunshots fired.

BOX 26-EMS-AMBULANCE STAND-BY ONE BLOCK FROM 2815 GOLDEN EAGLE DRIVE.

Rationale: This is the millenium, and lots of folks will be partying and doing 'stupid' things.

2325: SVPD dispatch sends a 'test' tone to all stations, and determines the radio system and CAD is back on-line.

2331: Power goes off in the entire city once again.
Rationale: Electrical power supply is unstable during this time period.

2340: SVPD receive a call via cellular phone that a citizen has their finger stuck in a champagne bottle at 59 James Pl NW.

BOX 11-EMS-PUBLIC ASSIST- 59 JAMES PL. NW.

Rationale: Some people do stupid things.

2355: A fire alarm activation occurs at Buena High School

BOX 21-ALARM ACTIVATION-BHS;

Rationale: same as earlier alarm activations.

0001: A caller from a cell phone states that he has put a bomb somewhere in SVRMC and hangs up.
BOX 16-EMS- PD REQUEST AN ENGINE AND AMBULANCE TO STAGE AT WILCOX AND EL CAMINO REAL FOR POSSIBLE BOMB AT SVRMC.

Rationale: This time frame is viewed by authorities as a prime-time for terrorism activity.

0012: SVPD receives a call via cellular phone that 'there is a bad accident at the BST and Hwy 92 intersection, with one car that has rolled over."

BOX 26-EMS-962 ROLLOVER-BST/92;
Rationale: No traffic signals functioning due to loss of power.

0051: A citizen calls via cellular and reports a brush fire threatening a structure in a vacant lot just east of North 7th on Tacoma. He states that he believes some New Year's revelers were lighting off bottle rockets and that is what caused the fire.

BOX 13-BRUSH FIRE THREATENING A STRUCTURE- TACOMA AND 7TH;
Rationale: Once again, a certain degree of stupidity should be expected during this time frame due to peoples brains not being "Y2K compliant."

0055: Fire units report on-scene that the brush fire has caught an exposure on fire (a storage shed) but have no hydrant pressure in that area.
Rationale: Loss of electricity causes loss of hydrant pressure. This is a grave concern expressed by Judy Gignac on several occasions.

0056: SVRHC calls and requests an ambulance to transfer a patient to Tucson from the Labor/Delivery; this is code 3 because of the loss of power and use of generator power at their facility.

BOX 16-EMS-TRANSFER-CODE 3-SVRHC TO TMC

Rationale: Many people are anxious to have their baby on the millenium; therefore an increase in births throughout late December into January can be expected.

0103: Another alarm activation occurs, this time at the Life Care Center
BOX 16-ALARM ACTIVATION-LIFE CARE CENTER
Rationale: Same as for earlier alarm activations.

0104: Alarm activation reported at Doss Moving and Storage

BOX 11-ALARM ACTIVATION-DOSS MOVING AND STORAGE

Rationale: same as above.

0105: Telephone service is restored to the entire city.

0144: SVPD receives a call for a child having an asthma attack at 105 Twilight Drive.

BOX 21-EMS-CHILD HAVING ASTHMA ATTACK-105 TWILIGHT DRIVE

Rationale: No Y2K relationship

0233: SVPD receives a call for a 'man down' in the parking lot of the Sorry Gulch Saloon.

BOX 12-EMS-UNCONSCIOUS PERSON-526 W. FRY BLVD.

Rationale: No Y2K relationship

0305: Power is restored to entire city

0603: CAD and radio in dispatch once again goes down.
Rationale: Y2K problems with circuitry and repeater tower.

0630: Fry Fire District and Ft. Huachuca call SVPD and inquire as to the status of the 911 system, as theirs are out of service temporarily.

END OF EXERCISE